PATENT APPLICATION
DOCKET NO. 200310639-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

INVENTOR(S):	Alan C. Berkema	**GROUP ART UNIT:**	2136
SERIAL NO.:	10/728,495	**EXAMINER:**	Hoang, Daniel L.
FILED:	12/05/2003	**CONFIRMATION NO:**	9731
SUBJECT:	DEVICE PAIRING		

COMMISSIONER FOR PATENTS
ALEXANDRIA, VA 22313-1450

SIR:

APPELLANTS'/APPLICANTS' OPENING BRIEF ON APPEAL

1. **REAL PARTY IN INTEREST.**

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holding, LLC.

2. **RELATED APPEALS AND INTERFERENCES.**

There are no other appeals or interferences known to Appellants, Appellants' legal representative or the Assignee which will affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. **STATUS OF CLAIMS.**

Claims 1, 2, 10-18, 21, 23-32, 40-49 are pending but stand rejected. Claims 28 and 29 have been cancelled. Claims 3-9, 14, 19, 20, 22, 27, 33-39, and 44 have been cancelled. The rejections of all pending claims are appealed.

4. **STATUS OF AMENDMENTS.**

No amendments have been filed after the final action was entered. All other previous amendments have been entered.

5. **SUMMARY OF CLAIMED SUBJECT MATTER.**

Claim 1 recites a method for publishing a PIN for use in establishing a pairing between a claimant device and a printing device. The method includes the printing device detecting a local PIN request made by activation of a user interface control element provided by the printing device. *See, e.g.*, Specification, paragraph [0049], page 11, lines 17-25, Figure 8, Step 130. The printing device generates the PIN in response to the local PIN request and without communicating with the claimant device. *See, e.g.*, Specification,

paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. The printing device prints the PIN. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. A connection request is received from the claimant device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 140. The connection request includes PIN data assembled from the PIN. *See, e.g.*, Specification, paragraphs [0052] and [0056], page 12, lines 3-8, page 13, lines 1-6, and Fig. 8, step 144. A link key is generated using the PIN data. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 146. The link key is used for device pairing between the claimant device and the printing device. *See, e.g.*, Specification, paragraphs [0016], page 12, lines 9-17.

Claim 13 recites a method for establishing a pairing between a claimant device and a verifying device. The method includes detecting a local PIN request made by activation of a user interface control element provided by the verifying device. *See, e.g.*, Specification, paragraph [0049], page 11, lines 17-25, Figure 8, Step 130. A PIN is generated in response to the local PIN request and without communicating with the claimant device. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. The verifying device is instructed to print the PIN. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. A connection request for the verifying device is received from the claimant device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 140. The connection request includes PIN data. *See, e.g.*, Specification, paragraphs [0052] and [0056], page 12, lines 3-8, page 13, lines 1-6, and Fig. 8, step 144. It is determined whether a link key exists for the verifying device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8, and Fig. 8, step 142. If a link key exists, the connection request is

rejected if the verifying device is not multi-claimant enabled. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 150. If a link key exists, the connection request is rejected if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 152. If a link key does not exist and upon a determination that the PIN data is valid, a link key is generated from the PIN data to establish a pairing between the claimant device and the verifying device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, steps 144 and 146.

Claim 17 recites a method for establishing a pairing between a claimant device and a printing device. The method includes detecting a local request to print a test page made by activation of a user interface control element provided by the printing device. *See, e.g.*, Specification, paragraph [0049], page 11, lines 17-25, Figure 8, Step 130. A PIN is generated in response to the local request to print the test page and without communicating with the claimant device. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. The printing device is instructed to print a test page that includes the PIN. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. A connection request is received from the claimant device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 140. The connection request includes PIN data. *See, e.g.*, Specification, paragraphs [0052] and [0056], page 12, lines 3-8, page 13, lines 1-6, and Fig. 8, step 144. It is determined whether a valid link key exists exist for the printing device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8, and Fig. 8, step 142. If a valid link key exists, the connection request is rejected if the verifying device is not multi-claimant enabled. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 150. If a link key exists, the connection

request is rejected if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 152. If a link key does not exist and upon a determination that the PIN data is valid, a link key is generated from the PIN data to establish a pairing between the claimant device and the printing device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 146.

Claim 18 recites a computer readable medium having instructions for implementing the method of claim 1. That method includes detecting a local PIN request made by activation of a user interface control element provided by the printing device. *See, e.g.*, Specification, paragraph [0049], page 11, lines 17-25, Figure 8, Step 130. The PIN is generated in response to the local PIN request and without communicating with the claimant device. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. The PIN is printed. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. A connection request is received from the claimant device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 140. The connection request includes PIN data assembled from the PIN. *See, e.g.*, Specification, paragraphs [0052] and [0056], page 12, lines 3-8, page 13, lines 1-6, and Fig. 8, step 144. A link key is generated using the PIN data. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 146. The link key is used for device pairing between the claimant device and the printing device. *See, e.g.*, Specification, paragraphs [0016], page 12, lines 9-17.:

Claim 26 recites a computer readable medium having instructions for: implementing the method of Claim 13. That method includes detecting a local PIN request made by activation of a user interface control element provided by the verifying device. *See, e.g.*, Specification, paragraph [0049], page 11, lines

17-25, Figure 8, Step 130. A PIN is generated in response to the local PIN request and without communicating with the claimant device. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. The verifying device is instructed to print the PIN. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. A connection request for the verifying device is received from the claimant device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 140. The connection request includes PIN data. *See, e.g.*, Specification, paragraphs [0052] and [0056], page 12, lines 3-8, page 13, lines 1-6, and Fig. 8, step 144. It is determined whether a link key exists for the verifying device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8, and Fig. 8, step 142. If a link key exists, the connection request is rejected if the verifying device is not multi-claimant enabled. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 150. If a link key exists, the connection request is rejected if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 152. If a link key does not exist and upon a determination that the PIN data is valid, a link key is generated from the PIN data to establish a pairing between the claimant device and the verifying device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, steps 144 and 146.

Claim 30 recites a computer readable medium having instructions for implementing the method of Claim 17. That method includes detecting a local request to print a test page made by activation of a user interface control element provided by the printing device. *See, e.g.*, Specification, paragraph [0049], page 11, lines 17-25, Figure 8, Step 130. A PIN is generated in response to the local request to print the test page and without communicating with the claimant device. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11,

lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. The printing device is instructed to print a test page that includes the PIN. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. A connection request is received from the claimant device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 140. The connection request includes PIN data. *See, e.g.*, Specification, paragraphs [0052] and [0056], page 12, lines 3-8, page 13, lines 1-6, and Fig. 8, step 144. It is determined whether a valid link key exists exist for the printing device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8, and Fig. 8, step 142. If a valid link key exists, the connection request is rejected if the verifying device is not multi-claimant enabled. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 150. If a link key exists, the connection request is rejected if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 152. If a link key does not exist and upon a determination that the PIN data is valid, a link key is generated from the PIN data to establish a pairing between the claimant device and the printing device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 146.

Claim 31 recites a system for publishing a PIN for use in establishing a pairing between a claimant device and a printing device. The system includes a PIN module, a publishing module, a connection module, an authentication module, and a key module. *See, e.g.*, Specification, paragraphs [0031]-[0034], page 6, line 23 through page 7, line 32 and Fig. 3, elements 76, 86, 84, 80, and 78. The pin module operable to receive a local PIN request made by activating a user interface control element provided by a verifying device. *See, e.g.*, Specification, paragraph [0034], page 7, lines 25-32. The pin module is operable to generate the PIN in response to the local PIN request and without communicating with the claimant device. *See, e.g.*, Specification, paragraph

[0034], page 7, lines 25-32. The publishing module is operable to direct a print engine for the printing device to print the PIN. *See, e.g.*, Specification, paragraph [0034], page 7, lines 25-32. The connection module operable to receive a connection request from the claimant device, the connection request including PIN data assembled from the PIN. *See, e.g.*, Specification, paragraph [0032], page 7, lines 6-18. The key module is operable to generate a link key using the PIN data, the link key used for paring the claimant device with the verifying device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, steps 144 and 146.

Claim 43 recites a system for establishing a pairing between a claimant device and a verifying device. The system includes a PIN module, a publishing module, a connection module, an authentication module, and a key module. *See, e.g.*, Specification, paragraphs [0031]-[0034], page 6, line 23 through page 7, line 32 and Fig. 3, elements 76, 86, 84, 80, and 78. The PIN module is operable to receive a local PIN request made by activating a user interface control element provided by a verifying device. *See, e.g.*, Specification, paragraph [0034], page 7, lines 25-32. The PIN module is operable to generate a PIN in response to the local PIN request and without communicating with a claimant device. *See, e.g.*, Specification, paragraph [0034], page 7, lines 25-32. The publishing module operable to instruct the verifying device to print the PIN. *See, e.g.*, Specification, paragraph [0034], page 7, lines 25-32. The connection module operable to receive from the claimant device a connection request that includes PIN data. *See, e.g.*, Specification, paragraph [0032], page 7, lines 6-18.

The authentication module is operable to implement a method that includes determining whether a link key exists for the verifying device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8, and Fig. 8, step 142. If a link key exists, the authentication module rejects the connection request if the verifying device is not multi-claimant enabled. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 150. If a link key exists, the authentication module rejects the connection request if the verifying device is

multi-claimant enabled with restricted access and the claimant device is not approved. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 152. The authentication module is also operable to determine the validity of the PID data and reject the connection request if the PIN data is not valid. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 144 and 148. The key module is operable to generate a link key is generated from the PIN data to establish a pairing between the claimant device and the verifying device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, steps 144 and 146.

Claim 47 recites a system for establishing a pairing between a claimant device and a printing device. The system includes a PIN module, a publishing module, a connection module, an authentication module, and a key module. *See, e.g.*, Specification, paragraphs [0031]-[0034], page 6, line 23 through page 7, line 32 and Fig. 3, elements 76, 86, 84, 80, and 78. The PIN module operable to receive a local request to print a test page made by activating a user interface control element provided by a printing device. *See, e.g.*, Specification, paragraph [0034], page 7, lines 25-32. The pin module is operable to generate a PIN in response to the local request to print the test page and without communicating with the claimant device. *See, e.g.*, Specification, paragraph [0034], page 7, lines 25-32. The publishing module is operable to instruct the printing device to print a test page that includes the PIN. *See, e.g.*, Specification, paragraph [0034], page 7, lines 25-32. The connection module is operable to receive from the claimant device a connection request that includes PIN data. *See, e.g.*, Specification, paragraph [0032], page 7, lines 6-18.

The authentication module is operable to implement a method that includes determining whether a link key exists for the verifying device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8, and Fig. 8, step 142. If a link key exists, the authentication module rejects the connection request if the verifying device is not multi-claimant enabled. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 150. If a link key exists,

the authentication module rejects the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 148 and 152. The authentication module is also operable to determine the validity of the PID data and reject the connection request if the PIN data is not valid. *See, e.g.*, Specification, paragraph [0052], page 12, lines 9-19, and Fig. 8, steps 144 and 148. The key module is operable to generate a link key is generated from the PIN data to establish a pairing between the claimant device and the verifying device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, steps 144 and 146.

Claim 48 recites a system for publishing a PIN for use in establishing a pairing between a claimant device and a printing device. The system includes various means for implementing a method. *See, e.g.*, Specification, paragraphs [0031]-[0034], page 6, line 23 through page 7, line 32 and Fig. 3, elements 76, 86, 84, 80, and 78. The PIN module operable to receive a local request to print a test page made by activating a user interface control element provided by a printing device. That method includes detecting a local PIN request made by activation of a user interface control element provided by the printing device. *See, e.g.*, Specification, paragraph [0049], page 11, lines 17-25, Figure 8, Step 130. A PIN is generated in response to the local PIN request and without communicating with the claimant device. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. The print engine is directed to print the PIN. *See, e.g.*, Specification, paragraphs [0049], [0051], and [0055], page 11, lines 17-25, page 11, line 31 through page 12, line 2, page 12, lines 27-32, and Fig. 8, step 138. A connection request is received from the claimant device. *See, e.g.*, Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 140. The connection request includes PIN data assembled from the PIN. *See, e.g.*, Specification, paragraphs [0052] and [0056], page 12, lines 3-8, page 13, lines 1-6, and Fig. 8, step 144. A link key is generated using the PIN data.

See, e.g., Specification, paragraphs [0052], page 12, lines 3-8 and Fig. 8, step 146. The link key is used for device pairing between the claimant device and the printing device. *See, e.g.*, Specification, paragraphs [0016], page 12, lines 9-17.

6. GROUNDS FOR REJECTION TO BE REVIEWED.

A. Claims 1, 2, 10-18, 21, 23-32, 40-49 stand rejected under 35 USC §112 first and second paragraphs.

B. Claims 1, 31, and 48 stand rejected under 35 U.S.C. §103 as being unpatentable over US Pub 2003/0065918 to Willey.

C. Claims 2, 10-12, 40-42, and 48 stand rejected under 35 U.S.C. §103 as being unpatentable over Willey in view of US Pub 2003/0105963 to Slick.

D. Claims 13, 15-18, 21, 23, 25, 26, 28-30, 31, 32, and 45-47 stand rejected under 35 U.S.C. §103 as being unpatentable over USPN 6,748,195 issued to Phillips.

7. ARGUMENT.

Grounds For Rejection A – Claims 1, 2, 10-18, 21, 23-32, 40-49 stand rejected under 35 USC §112 first and second paragraphs.

Claim 1, and the other independent claims, recite "generating the PIN in response to the local PIN request and without communicating with the claimant device." The Examiner contends that this limitation is not "described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to
make and/or use the invention." The Examiner further contends that the inclusion of the limitation renders the claims indefinite. In particular, the Examiner states

that based on the disclosure "communication is necessary." The Appellant respectfully disagrees.

Paragraphs [0034], [0049], and [0051] of the Specification are reproduced below:

> **[0034]** Referring back to Fig. 2, publishing module 86 may be part of print control logic 56. For example, publishing module 86 might be a program capable of directing print engine 52 to print a test page that includes a PIN generated by PIN module 76. In this case verifying device 40 will include a button or buttons that, when properly pressed, direct verifying device 40 to print a test page. In doing so, publishing module 86 informs security logic 60 that a test page has been requested. PIN module 76 generates and supplies publishing module 86 with a PIN. Publishing module 86 then directs print engine 52 to print a test page that includes the PIN.
>
> . . .
>
> **[0049]** A verifying device is powered on (step 126). The verifying device initializes and runs two processes. The verifying device waits for a connection request with a link key (step 128) – the receipt of which triggers the execution of the first process. The verifying device also waits for a local PIN request (step 130), the receipt of which triggers the second process. A local pin request is a request made using a button or other user interface control element provided by the verifying device. For example, the verifying device might include a button that when pressed directs the device to publish a PIN. An example of a non-local PIN request is a request that originates from a device other than the verifying device.
>
> . . .
>
> **[0051]** Upon receiving a local pin request (step 130), the verifying device generates and publishes a PIN (step 138). The generated PIN may, for example, be associated with expiration data and access data. The published PIN is entered by a user into a claimant device. The claimant device generates PIN data and directs a connection request that includes the PIN data to the verifying device.

Specification, paragraphs [0034], [0049], and [0051].

Paragraph [0034] expressly states that "verifying device 40 will include a button or buttons that, when properly pressed, direct verifying device 40 to print a test page." When that button is pressed, "PIN module 76 generates and supplies publishing module 86 with a PIN." Paragraph [0034] clearly describes the generation of a PIN by a verifying device where that verifying device does so "without communicating with the claimant device." In the example of paragraph [0034], the PIN is generated as a result of pressing a button on the verifying device. The claimant device plays no role I generating the PIN.

Paragraph [0049] describes a local PIN request as "a request made using a button or other user interface control element provided by the verifying device." Paragraph [0051] describes a verifying device generating a PIN upon receiving a local pin request. Once again, paragraphs [0049] and [0051] clearly describe the generation of a PIN by a verifying device where that verifying device does so "without communicating with the claimant device." In the example of paragraphs [0049] and [0051], the PIN is generated as a result of pressing a button on the verifying device. The claimant device plays no role in generating the PIN.

The Appellant respectfully maintains that the Specification provides more than adequate support for including the limitation "generating the PIN in response to the local PIN request and without communicating with the claimant device." For at least these reasons, the Appellant asks that the rejection under §112 be withdrawn.

Grounds For Rejection B – Claims 1, 31, and 48 stand rejected under 35 U.S.C. §103 as being unpatentable over US Pub 2003/0065918 to Willey.

It is initially noted that in making the §103 rejection, the Examiner notes at pages 2 and 3 of the final office action that he is interpreting the Claims as not including the limitation of generating a PIN without communicating with the claimant device. For the reasons set forth above, the Examiner's interpretation is flawed. As such, the Examiner's basis for rejecting Claims 1, 31, and 48 is also flawed.

Claim 1 is directed to a method for publishing a PIN for use in establishing a pairing between a claimant device and a printing device and, as amended, recites the following:

1. the printing device detecting a local PIN request made by activation of a user interface control element provided by the printing device;
2. the printing device generating the PIN in response to the local PIN request and without communicating with the claimant device;
3. the printing device printing the PIN;
4. receiving a connection request from the claimant device, the connection request including PIN data assembled from the PIN; and
5. generating a link key using the PIN data, the link key used for device pairing between the claimant device and the printing device.

The Appellant respectfully maintains that Willey fails to teach or suggest a printing device generating a PIN in response to a local PIN request where the PN is generated without communicating with the claimant device.

Willey describes a method for pairing a telephone with a headset. *See* Willey, Fig. 5a. A user initiates the pairing process via the user interface of the telephone. Willey, paragraph [0038]. In this case the telephone is a claimant device seeking to be paired with the headset –that is – the verifying device. The headset accepts the pairing request with or without confirmation. Willey, paragraph [0038]. The headset sends a confirmation signal to the telephone. Willey, paragraph [0039]. The telephone and the headset then exchange public keys. Willey, paragraph [0040]. The headset and the telephone use the keys to generate a shared secret. Willey, paragraph [0040]. That shared secret is used by each device to create a shared symmetric key. Willey, paragraph [0040]. Each device can then be converted to a decimal with a set number of least significant digits to generate a PIN. Willey, paragraph [0041]. To ensure the headset and the telephone have each generated the same PIN, the telephone displays the PIN on its user interface while the headset produces audible sounds

for each digit. Willey, paragraph [0042].

To summarize, the generation of a PIN, according to Willey, is initiated by a claimant device (telephone) and requires the claimant device and the verifying device (headset) to exchange data allowing each device to simultaneously generate the same PIN. Thus, Willey's verifying device does **not** generate a PIN in response to a local PIN request and without communicating with the claimant device.

Consequently, Willey fails to teach or suggest a method that includes: (a) the printing device detecting a local PIN request made by activation of a user interface control element provided by the printing device and (b) the printing device generating the PIN in response to the local PIN request and without communicating with the claimant device. For at least this reason, Claim 1 is patentable over Willy as are Claims 2 and 10-12 which depend from Claim 1.

Claim 31 is directed to a system for publishing a PIN for use in establishing a pairing between a claimant device and a printing device and, as amended, recites components operable to implement the method of Claim 1. In particular, Claim 31 recites a pin module that is operable to receive a local PIN request made by activating a user interface control element provided by a verifying device. The pin module is also operable to generate the PIN in response to the local PIN request and without communicating with a claimant device. As with Claim 1, Willey fails to teach or suggest generating a PIN in such a manner. For at least the same reasons Claim 1 is patentable, so are Claim 31 and Claims 32 and 40-42 which depend from Claim 31.

Claim 48 is directed to a system for publishing a PIN for use in establishing a pairing between a claimant device and a printing device. Claim 48 recites various means for implementing the method of Claim 1. For at least the same reasons Claim 1 is patentable, so are Claim 48 and Claim 49 which depends from Claim 48..

Grounds For Rejection C – Claims 2, 10-12, 40-42, and 48 stand rejected under 35 U.S.C. §103 as being unpatentable over Willey in view of US Pub 2003/0105963 to Slick.

It is initially noted that in making the §103 rejection, the Examiner notes at pages 2 and 3 of the final office action that he is interpreting the Claims as not including the limitation of generating a PIN without communicating with the claimant device. For the reasons set forth above, the Examiner's interpretation is flawed. As such, the Examiner's basis for rejecting Claims 2, 10-12, 40-42, and 48 is also flawed.

Claims 2 and 10-12 depend from Claim 1 and include all the limitations of that base Claim. For at least the same reasons Claim 1 is patentable, so are Claims 2 and 10-12.

Claims 40-42 depend from Claim 31 and include all the limitations of that base Claim. For at least the same reasons Claim 31 is patentable, so are Claims 40-42.

Claim 48 is directed to a system that includes various means for implementing the method of Claim 1. For at least the same reasons Claim 1 is patentable, so are Claims 48 and Claim 49 which depends from Claim 48.

Grounds For Rejection D – Claims 13, 15-18, 21, 23, 25, 26, 28-30, 31, 32, and 45-47 stand rejected under 35 U.S.C. §103 as being unpatentable over USPN 6,748,195 issued to Phillips.

It is initially noted that in making the §103 rejection, the Examiner notes at pages 2 and 3 of the final office action that he is interpreting the Claims as not including the limitation of generating a PIN without communicating with the claimant device. For the reasons set forth above, the Examiner's interpretation is flawed. As such, the Examiner's basis for rejecting Claims , 15-18, 21, 23, 25, 26, 28-30, 31, 32, and 45-47 is also flawed.

Claim 13 is directed to a method for establishing a pairing between a claimant device and a verifying device and recites the following:

1. detecting a local PIN request made by activation of a user interface control element provided by the verifying device;
2. generating a PIN in response to the local PIN request and without communicating with the claimant device;
3. instructing the verifying device to print the PIN;
4. receiving from the claimant device a connection request for the verifying device, the connection request including PIN data;
5. determining whether a link key exists for the verifying device;
6. if a link key exists:
    a. rejecting the connection request if the verifying device is not multi-claimant enabled;
    b. rejecting the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved;
7. otherwise, upon a determination that the PIN data is valid, generating a link key from the PIN data to establish a pairing between the claimant device and the verifying device.

Claim 13 – *not unlike Claim 1* – recites (a) detecting a local PIN request made by activation of a user interface control element provided by the verifying device and (b) generating a PIN in response to the local PIN request and without communicating with the claimant device. This is not taught or suggested by Phillips. .

Addressing Claim 13, the Examiner cites Phillips col. 7, lines 3-17. This passage is reproduced below:

> FIG. 6 is a table that defines exemplary profile parameters being associated with the profile A at the home location. At home, the wireless device **12** can be enabled to communicate with certain home devices, such as personal printer, personal computer, but not with neighboring devices, with low level security. FIG. 7 is a table that defines exemplary parameters being associated with the profile B at the office location, where the wireless device can be set to communicate with office printers, network devices, other computers, with moderate level security. However, when the wireless devices is out of the office, the device can be disabled to communicate with peer devices for security reasons and for conservation of resources, and other reasons. FIG. 8 is a table that defines exemplary parameters being associated with the profile C at the second location, which is everywhere else.

Phillips, col. 7, lines 3-18.

Phillips mentions nothing of a verifying device generating a PIN in response to the detection of a local PIN request made by activation of a user interface control element provided by the verifying device. Furthermore Phillips mentions nothing of generating a PIN without communicating with a claimant device.

For at least the same reasons Claim 1 is patentable, so are Claim 13 and Claims 15 and 16 which depend from Claim 13.

Claim 17 recites a method that includes (a) detecting a local request to print a test page made by activation of a user interface control element provided by the printing device and (b) generating a PIN in response to the local request to print the test page and without communicating with the claimant device. As explained with respect to Claims 1 and 13 above, Phillips and Willey neither teach nor suggest generating a PIN in response to the detection of such a request or generating a PIN without communicating with the claimant device. For at least the same reasons Claims 1 and 13 are patentable, so is Claim 17.

Claim 18 is directed to a computer readable medium. The medium includes instructions for implementing the method of Claim 1. As explained with respect to Claims 1 and 13 above, Willey and Phillips fail to teach or suggest

detecting a local PIN request made by activation of a user interface control element provided by the printing device and generating the PIN in response to the local PIN request and without communicating with the claimant device. For at least the same reasons Claims 1 and 13 are patentable, so are Claim 18 and Claim 21 and Claims 23-25 which depend from Claim 18.

Claim 26 is directed to a computer readable medium having instructions for implementing the method of Claim 13. For at least the same reasons Claim 13 is patentable, so are Claim 26 and Claims 28 and 29 which depend from Claim 26.

Claim 30 is directed to a computer readable medium having instructions for implementing the method of Claim 17. For at least the same reasons Claim 17 is patentable (addressed below), so are Claim 30 and Claim 31 which depends from Claim 30.

Claim 32 depends from Claim 31, For at least the same reasons Claim 31 is patentable, so is Claim 32.

Claim 43 is directed to a system having components for implementing the method of Claim 13. For at least the same reasons Claim 13 is patentable, so are Claim 43 and Claims 45 and 46 which depend from Claim 43.

Claim 47recites a system that includes various components configured to implement the method of Claim 17. For at least the same reasons Claim 17 is patentable, so is Claim 47.

Conclusion

In view of the foregoing remarks and amendments, the Appellant respectfully submits that Claims 1, 2, 10-18, 21, 23-32, and 40-49 define allowable subject matter.

Respectfully submitted,
Alan C. Berkema

By /Jack H. McKinney/
Jack H. McKinney
Reg. No. 45,685

August 20, 2008

APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

1. (previously presented) A method for publishing a PIN for use in establishing a pairing between a claimant device and a printing device, comprising:

the printing device detecting a local PIN request made by activation of a user interface control element provided by the printing device;

the printing device generating the PIN in response to the local PIN request and without communicating with the claimant device;

the printing device printing the PIN;

receiving a connection request from the claimant device, the connection request including PIN data assembled from the PIN; and

generating a link key using the PIN data, the link key used for device pairing between the claimant device and the printing device.

2. (original) The method of Claim 1, identifying a local request to print a test page as the local PIN request and wherein printing the PIN comprises printing a test page that includes the PIN.

3. (cancelled)

4. (cancelled)

5. (cancelled)

6. (cancelled)

7. (cancelled)

8. (cancelled)

9. (cancelled)

10. (previously presented) The method of Claim 1, further comprising determining the validity of the PIN data prior to generating the link key.

11. (original) The method of Claim 10, wherein determining includes determining if the PIN data corresponds to the PIN, determining if the generated PIN has expired, and rejecting the connection request if the PIN data does not correspond to the PIN or if the PIN has expired.

12. (previously presented) The method of Claim 1, further comprising rejecting the connection request if the connection request is for a function not associated with the PIN data.

13. (previously presented) A method for establishing a pairing between a claimant device and a verifying device, comprising:

detecting a local PIN request made by activation of a user interface control element provided by the verifying device;

generating a PIN in response to the local PIN request and without communicating with the claimant device;

instructing the verifying device to print the PIN;

receiving from the claimant device a connection request for the verifying device, the connection request including PIN data;

determining whether a link key exists for the verifying device;

if a link key exists:

rejecting the connection request if the verifying device is not multi-claimant enabled;

rejecting the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved;

otherwise, upon a determination that the PIN data is valid, generating a

link key from the PIN data to establish a pairing between the claimant device and the verifying device.

14. (cancelled)

15. (previously presented) The method of Claim 13, wherein the PIN and the PIN data are of the same format and wherein determining the validity of the PIN data includes determining if the PIN data matches the generated PIN.

16. (previously presented) The method of Claim 13, wherein determining the validity of the PIN data comprises:

acquiring a unique identifier for the claimant device;

constructing verifying PIN data using the unique identifier and the generated PIN;

determining if the PIN data matches the verifying PIN data.

17. (previously presented) A method for establishing a pairing between a claimant device and a printing device, comprising:

detecting a local request to print a test page made by activation of a user interface control element provided by the printing device;

generating a PIN in response to the local request to print the test page and without communicating with the claimant device;

instructing the printing device to print a test page that includes the PIN;

receiving from the claimant device a connection request, the connection request including PIN data;

determining whether a valid link key exists exist for the printing device;

if a valid link key exists:

rejecting the connection request if the printing device is not multi-claimant enabled;

rejecting the connection request if the printing device is multi-claimant enabled with restricted access and the claimant device is

not approved;

otherwise, upon a determination that the PIN data is valid, generating a link key from the PIN data to establish a pairing between the claimant device and the printing device.

18. (previously presented) A computer readable medium having instructions for:

detecting a local PIN request made by activation of a user interface control element provided by a printing device;

generating a PIN in response to a local PIN request and without communicating with the claimant device;

printing the PIN;

receiving a connection request from the claimant device, the connection request including PIN data assembled from the PIN; and

generating a link key using the PIN data to establish a device pairing between the printing device and the claimant device.

19. (cancelled)

20. (cancelled)

21. (previously presented) The medium of Claim 18, wherein the local PIN request is a local request to print a test page, and wherein the instructions for printing include instructions for printing a test page that includes the PIN.

22. (cancelled)

23. (original) The medium of Claim 18, having further instructions for determining the validity of the PIN data prior to generating the link key.

24. (original) The medium of Claim 23, wherein the instructions for determining include instructions for determining if the PIN data corresponds to the PIN, determining if the generated PIN has expired, and rejecting the connection request if the PIN data does not correspond to the PIN or if the PIN has expired.

25. (original) The medium of Claim 18, having further instructions for rejecting the connection request if the connection request is for a function not associated with the PIN data.

26. (previously presented) A computer readable medium having instructions for:

detecting a local PIN request made by activation of a user interface control element provided by a verifying device;

generating a PIN in response to a local PIN request and without communicating with the claimant device;

instructing the verifying device to print the PIN;

receiving from a claimant device a connection request, the connection request including PIN data;

determining whether a link key exists for a verifying device;

if a link key exists:

rejecting the connection request if the verifying device is not multi-claimant enabled;

rejecting the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved;

otherwise, upon a determination that the PIN data is valid, generating a link key from the PIN data to establish a pairing between the claimant device and the verifying device.

27. (cancelled)

28. (previously presented) The medium of Claim 26, wherein the PIN and the PIN data are of the same format and wherein the instructions for determining the validity of the PIN data include instructions for determining if the PIN data matches the generated PIN.

29. (previously presented) The medium of Claim 26, wherein the instructions for determining the validity of the PIN data include:

acquiring a unique identifier for the claimant device;

constructing verifying PIN data using the unique identifier and the generated PIN;

determining if the PIN data matches the verifying PIN data.

30. (previously presented) A computer readable medium having instructions for:

detecting a local request to print a test page made by activation of a user interface control element provided by a printing device;

generating a PIN in response to local request to print a test page and without communicating with the claimant device;

instructing the printing device to print a test page that includes the PIN;

receiving from a claimant device a connection request, the connection request including PIN data;

determining whether a valid link key exists for the printing device;

if a valid link key exists:

rejecting the connection request if the printing device is not multi-claimant enabled;

rejecting the connection request if the printing device is multi-claimant enabled with restricted access, and the claimant device is not approved;

otherwise, upon a determination that the PIN data is valid, generating a link key from the PIN data to establish a pairing between the claimant device and the printing device.

31. (previously presented) A system for publishing a PIN for use in establishing a pairing between a claimant device and a printing device, comprising:

a pin module operable to receive a local PIN request made by activating a user interface control element provided by a verifying device, the pin module being operable to generate the PIN in response to the local PIN request and without communicating with the claimant device;

a publishing module operable to direct a print engine for the printing device to print the PIN;

a connection module operable to receive a connection request from the claimant device, the connection request including PIN data assembled from the PIN; and

a key module operable to generate a link key using the PIN data, the link key used for paring the claimant device with the verifying device.

32. (original) The system of Claim 31, wherein the local PIN request is a local request to print a test page, and wherein the publishing module is operable to identify the request, to direct the PIN module to generate the PIN, and to direct the print engine to print a test page that includes the PIN.

33. (cancelled)

34. (cancelled)

35. (cancelled)

36. (cancelled)

37. (cancelled)

38. (cancelled)

39. (cancelled)

40. (currently amended) The system of Claim 31, further comprising an authentication module operable to validate the PIN data and to instruct the key module to generate a link key upon a determination that the PIN data is valid.

41. (original) The system of Claim 40, wherein the authentication module is operable to determine if the PIN data corresponds to the PIN, to determine if the generated PIN has expired, and to reject the connection request if the PIN data does not correspond to the PIN or if the PIN has expired.

42. (currently amended) The system of Claim 31, further comprising an authentication module operable to reject the connection request if the connection request is for a function not associated with the PIN data.

43. (previously presented) A system for establishing a pairing between a claimant device and a verifying device, comprising:

a PIN module operable to receive a local PIN request made by activating a user interface control element provided by a verifying device, the pin module being operable to generate a PIN in response to the local PIN request and without communicating with a claimant device;

a publishing module operable to instructing the verifying device to print the PIN;

a connection module operable to receive from the claimant device a connection request, the connection request including PIN data;

an authentication module operable:

to determine whether a valid link key exists for the verifying device;

to reject the connection request if the verifying device is not multi-claimant enabled and a valid link key exists;

to reject the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved;

to determine the validity of the PIN data and reject the connection request upon a determination that the PIN data is not valid; and

a key module operable to generate a link key from the PIN data to establish a pairing between the claimant device and the verifying device.

44. (cancelled)

45. (previously presented) The system of Claim 43, wherein the PIN and the PIN data are of the same format and wherein the authentication module is operable to determine the validity of the PIN data by determining if the PIN data matches the generated PIN.

46. (previously presented) The system of Claim 43, wherein the authentication module is operable to validate the PIN data by:

acquiring a unique identifier for the claimant device;

constructing verifying PIN data using the unique identifier and the generated PIN;

determining if the PIN data matches the verifying PIN data.

47. (previously presented) A system for establishing a pairing between a claimant device and a printing device, comprising:

a PIN module operable to receive a local request to print a test page made by activating a user interface control element provided by a printing device, the

pin module being operable to generate a PIN in response to the local request to print the test page and without communicating with the claimant device;

a publishing module operable to instruct the printing device to print a test page that includes the PIN;

a connection module operable to receive from the claimant device a connection request, the connection request including PIN data;

an authentication module operable:

to determine whether a link key exists for the verifying device and if a link key exists;

to reject the connection request if the verifying device is not multi-claimant enabled;

to reject the connection request if the verifying device is multi-claimant enabled with restricted access and the claimant device is not approved;

to determine the validity of the PIN data and reject the connection request if the PIN data is not determined to be valid; and

a key module operable to generate a link key from the PIN data to establish a pairing between the claimant device and the verifying device.

48. (previously presented) A system for publishing a PIN for use in establishing a pairing between a claimant device and a printing device, comprising:

a means for identifying a local PIN request made by activation of a user interface control element provided by the printing device ;

a means for generating the PIN in response to the local PIN request and without communicating with the claimant device;

a means for directing a print engine for the printing device to print the PIN

a means for receiving a connection request from the claimant device, the connection request including PIN data assembled from the PIN; and

a means for generating a link key using the PIN data, the link key used for device pairing between the claimant device and the printing device.

49. (original) The system of Claim 48, wherein the means for identifying is a means for identifying a local request to print a test page, and wherein the means for directing is a means for directing the print engine to print a test page that includes the PIN.

Evidence Appendix

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix

There are no related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.